MCR Decoding: A MIMO Approach for Defending Against Wireless Jamming Attacks

Wenbo Shen*, Peng Ning*, Xiaofan He*, Huaiyu Dai* and Yao Liu†
* North Carolina State University, {wshen3, xhe6, hdai, pning}@ncsu.edu
† University of South Florida, yliu@cse.usf.edu

Abstract—**This paper presents a novel technique - *Multi-Channel Ratio (MCR) Decoding*, which aims at providing an anti-jamming wireless communication capability for multi-antenna wireless devices. The basic idea of MCR decoding is to fully leverage the repeated preamble signals and the multi-channel characteristics in MIMO communications to detect and recover the desired transmission signals under constant and reactive jamming attacks. This paper also reports the analysis, implementation, and experimental evaluations of MCR decoding on a software-defined radio platform - GNURadio and USRP, which show that the proposed MCR decoding can detect the desired transmission reliably under the jamming attack and remove jamming signals effectively in the real world environment.**

I. Introduction

Due to the shared use of the wireless medium, wireless applications are vulnerable to jamming attacks. A jammer can simply emit random noise to disrupt wireless communications between the transmitter and the receiver. Therefore, the robustness against jamming attacks is crucial for wireless applications which require high communication reliability.

Spread spectrum techniques such as direct-sequence spread spectrum (DSSS), frequency-hopping spread spectrum (FHSS) and their enhanced variations, including the DSSS variations [10], [11], [15] and FHSS variations [9], [18], are commonly used techniques for anti-jamming wireless communications. However, these spread spectrum based schemes require large spectrum bandwidth, which is undesirable considering the scarcity of the wireless spectrum.

The recent advances of multiple-input and multiple-out (MIMO) technique [4] bring new hope for enhancing anti-jamming wireless communications. In particular, research groups have investigated the MIMO systems for interference cancellation. Gollakota et al. proposed the Technology Independent Multi-Output (TIMO) scheme [6], which exploits the channel ratio (the ratio of channel coefficients) of the interference source and the transmitter's channel state information (a.k.a. channel coefficient) to remove cross-technology interference for 802.11n wireless networks. Due to the requirement of the transmitter's channel state information, TIMO cannot deal with the fast reactive jamming attacks. Under the fast reactive jamming attack, the jamming signals start and stop at almost the same time with the desired transmission signals. The receiver has neither enough un-jammed preamble signals to estimate the transmitter's channel state information, nor pure jamming signals to compute channel ratio of the jammer, and thus it cannot remove the jamming signals. Moreover, TIMO is only capable of removing interference from single interference source, which is reasonable for dealing with unintended interference. However, for intended adversarial jammers, it is very likely that multiple jammers operate on the same frequency.

To address these problems, we extend the TIMO technique into the anti-jamming domain and propose an anti-jamming technique, *Multi-Channel Ratio (MCR) Decoding*, which exploits the multi-channel ratio (i.e., the ratio of two channel coefficients) and the repeated preamble signals to detect and recover the desired transmission signals under constant and reactive jamming attacks.

Unlike the spread spectrum schemes which suppress the jamming signals at the price of spectrum bandwidth, MCR decoding exploits the MCR to subtract the jamming signals directly. Moreover, MCR decoding does not require any shared keys to build its anti-jamming capability. Hence, it does not suffer from the vulnerabilities introduced by the shared keys.

Compared with TIMO, MCR decoding eliminates the need of the transmitter's channel state information, which makes it more suitable for anti-jamming applications. MCR decoding uses the multi-channel ratio to detect the transmissions under jamming attacks and can handle multiple constant jammers on the same frequency band as well as the fast reactive jammer, even though the reactive jamming signals start and stop at the same time with the desired transmission signals.

The contributions of this paper are two-fold. First, we identify the limitations of applying the TIMO technique into the anti-jamming domain and propose MCR decoding which can detect and recover the desired transmission signals under jamming attacks. Second, we have implemented a prototype for MCR decoding based on the GNURadio [1] and Universal Software Radio Peripheral (USRP) [12], and performed extensive experimental evaluations. Our experimental results show that MCR decoding can detect the desired transmission accurately under the jamming attack and remove more than 99.86% of the jamming signal power.

II. Preliminaries

A. Wireless Communication Systems

Wireless communication systems generally use radio frequency (RF) signals to convey information. Upon receiving

This work was supported in part by the National Science Foundation under Grants CNS-1016260 and ECCS-1307949.

bits from upper layers, the transmitter first maps them to *discrete base-band signals* (a.k.a. *physical layer symbols*), then converts these discrete signals to analog signals, and finally up-converts them to RF signals [17].

The RF signals go through the wireless channel before being received by the receiver. The wireless channel introduces attenuation, phase shift, and noise during transmission. The hardware of the transmitter and the receiver introduces the frequency offset Δf [7]. Thus after the signal $x(i)$ is transmitted through the channel, it is transformed into the received signal $y(i)$, and

$$y(i) = he^{j2\pi\Delta f t_i}x(i) + n(i)^1,$$

where h is a complex number, containing *channel attenuation* and *phase shift*, $e^{j2\pi\Delta f t_i}$ is a complex number in its polar form (i.e., a complex number $a+bj$ can be represented by its polar form $Me^{j\theta}$, where $M = \sqrt{a^2+b^2}$ and $\theta = \tan^{-1}(b/a)$ [13]), $n(i)$ is the *noise* and t_i is the sampling time for sample $y(i)$; $y(i)$ and $x(i)$ are discrete base-band signals, which can also be represented by complex numbers.

Even though channel effects and the frequency offset are unknown, the receiver can use the phase-locked loop to compensate Δf, and use differential encoding schemes to tolerate the phase shift. Therefore, it can recover the transmitted signal $x(i)$ by using existing synchronization approaches [5], [8], [16]. Then the receiver can de-map the physical layer symbol $x(i)$ to bits and recover the transmitted message.

B. MIMO Systems

In a MIMO system, if both transmitting and receiving antennas are separated properly, the channel between each transmitting and receiving antennas pair will be different from each other [19]. Consider a 2 × 2 MIMO system shown in Fig. 1, the transmitter sends signals of two packets, x_1 on Antenna 1, x_2 on Antenna 2 concurrently, the receiver will receive

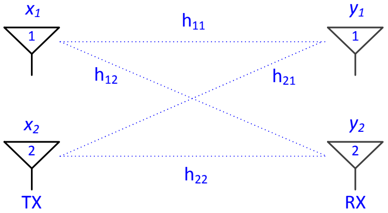

Fig. 1. A 2 ×2 MIMO system. h_{ij} is the channel coefficient for transmitter antenna i and receiver antenna j, include channel attenuation and phase shift.

$$\begin{cases} y_1(i) = h_{11}\cdot x_1(i) + h_{21}\cdot x_2(i) + n_1(i) \\ y_2(i) = h_{12}\cdot x_1(i) + h_{22}\cdot x_2(i) + n_2(i) \end{cases},$$

where $y_m(i)$ is the signal received by the mth antenna of the receiver, $n_1(i)$ and $n_2(i)$ are the white noise. As the signal to noise ratio (SNR) is high enough, if the receiver knows the channel coefficients h_{ij}, it can solve the above equations (two equations and two unknowns $x_1(i)$ and $x_2(i)$) to decode the concurrently transmitted packets.

To let the receiver compute the channel coefficients, the MIMO transmitter starts each frame by transmitting a known preamble from each of its antennas, one after the other [6]. By combining the knowledge of both the received and the transmitted preamble signals, the receiver can compute the channel coefficients, which can be used to decode the packet signals of this frame [3], [14]. However, if the jammer jams the preamble, the received preamble signals will be totally disrupted by the jamming signals, which will lead to wrong estimations of the channel coefficients. As a result, the received signals cannot be decoded.

III. Assumptions and Threat Model

A. Assumptions

We assume that the wireless channels are single-tap. As the receiver needs and both the received transmission signals and the received jamming signals at the receiver have a sufficient signal to noise ratio (SNR). We assume all devices, including the transmitter, the receiver and the jammer, are immobile, hence, channels between them do not change significantly in a short period. Finally, we assume the receiver has at least two antennas while the jammer and the transmitter have single antenna. We will generalize MCR decoding for the multi-antenna jammer in our future work.

B. Threat Model

The objective of the jammer is to defeat the proposed scheme to disable the legal wireless transmissions. MCR only depends on the channel coefficients, rather than the jamming signals, which makes it only sensitive to whether the jamming is on or not. The jammer can use different strategies to jam channel. According to the jamming strategies, we classify the jammers into three categories: the constant jammer, the random on-off jammer and the reactive jammer.

The constant jammer emits random jamming signals all the time. The random on-off jammer jams the channel or keeps silent for random intervals. The reactive jammer listens to the channel and transmits jamming signals when an ongoing communication is detected.

The anti-jamming scheme and the analysis of MCR decoding for the constant jammer and the random on-off jammer are roughly the same. For brevity, we only consider the constant jammer and reactive jammer in the following sections.

IV. MCR Decoding

In this section, we first give an overview of MCR decoding, then discuss the techniques against the constant jammer and the reactive jammer.

A. System Overview

The basic idea of MCR decoding is to exploit the channel ratio of the jammer (i.e., the ratio of two channel coefficients) to remove the jamming signals, then use certain techniques such as differential encoding, phase-locked loop to recover the

[1] This equation is for single-tap channels.

desired transmission signals. Let us use the scenario shown in Fig. 2 to illustrate the process. The receiver does not know the jammer's channels h_{11} and h_{12}. Under the jamming attack, the receiver cannot even estimate the transmitter's channels h_{21} and h_{22}. Therefore, the traditional MIMO approaches cannot be applied to recover the transmitter's signals under the jamming attack even though the receiver has two antennas.

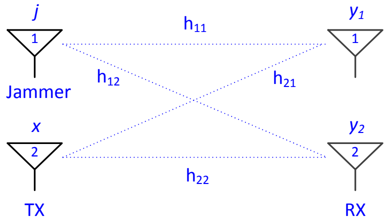

Fig. 2. A scenario with the jammer. The transmitter TX and the jammer are single-antenna devices, the receiver RX is a bi-antenna device.

To defend against the jamming attacks, MCR decoding uses the multi-channel ratio (MCR) to remove the jamming signals. Here we assume the jammer is a constant jammer and defer the discussion on the reactive jammer case to later sections. Assume the transmitter is silent, the jammer is jamming and for the jamming signal $j(i)$ emitted by the jammer, the received signal by receiver's two antennas are $y_1(i)$ and $y_2(i)$ respectively, ignoring the white noise, we have

$$\begin{cases} y_1(i) = h_{11}e^{j2\pi\Delta f_j t_i} \cdot j(i) \\ y_2(i) = h_{12}e^{j2\pi\Delta f_j t_i} \cdot j(i) \end{cases},$$

where Δf_j is the frequency offset between the receiver and the jammer[2] and t_i is the sampling time. We use φ to represent the MCR of the two channels between the receiver and the jammer, and thus

$$\varphi(i) = \frac{h_{11}}{h_{12}} = \frac{y_1(i)}{y_2(i)}. \tag{1}$$

It is worth noting that φ does not rely on the jamming signals. In other words, if the jammer and the receiver do not move, φ should remain the same over a short period time (e.g., several ms).

Then when the transmission is being jammed, assume the transmitter TX is transmitting signal $x(k)$, while the jammer is emitting signal $j(k)$, the received signals from the two antennas are $y_1(k)$, $y_2(k)$ respectively, we have

$$\begin{cases} y_1(k) = h_{11}e^{j2\pi\Delta f_j t_k} \cdot j(k) + h_{21}e^{j2\pi\Delta f t_k} \cdot x(k) \\ y_2(k) = h_{12}e^{j2\pi\Delta f_j t_k} \cdot j(k) + h_{22}e^{j2\pi\Delta f t_k} \cdot x(k) \end{cases}. \tag{2}$$

As φ remains the same for a short time, we can replace h_{11} in Equation (2) with $\varphi(i)$ and h_{12} so that

$$\begin{cases} y_1(k) = h_{12}e^{j2\pi\Delta f_j t_k} j(k) \cdot \varphi(i) + h_{21}e^{j2\pi\Delta f t_k} x(k) \\ y_2(k) = h_{12}e^{j2\pi\Delta f_j t_k} j(k) + h_{22}e^{j2\pi\Delta f t_k} x(k) \end{cases}.$$

As the value of $\varphi(i)$ is known, the receiver can treat $h_{12}e^{j2\pi\Delta f_j t_k} j(k)$ as one unknown and subtract it from $y_1(k)$ or $y_2(k)$, then it follows that

$$[\varphi(i) \cdot h_{22} - h_{21}]e^{j2\pi\Delta f t_k} x(k) = \varphi(i)y_2(k) - y_1(k),$$

where $y_1(k)$, $y_2(k)$ and $\varphi(i)$ are known. Even though h_{21} and h_{22} are unknown, the receiver can treat $[\varphi(i) \cdot h_{22} - h_{21}]e^{j2\pi\Delta f}$ as the new channel coefficient so that it can use phase-locked loop to compensate the effect of $e^{j2\pi\Delta f}$. The differential encoding at both the transmitter and the receiver can tolerate the phase shift introduced by $\varphi(i) \cdot h_{22} - h_{21}$. Therefore, by regarding $[\varphi(i) \cdot h_{22} - h_{21}]e^{j2\pi\Delta f}$ as the new, unknown channel efficient, the receiver can tolerate its impacts and recover $x(k)$ under the jamming attack.

B. Transmission Detection

To reduce the work load, the receiver only needs to perform MCR decoding when it detects the being jammed transmissions. Therefore, it needs to be able to detect the ongoing transmissions under the jamming attack. It turns out that this problem can be solved by monitoring MCR values, and we term this technique as *MCR Detection*. To simplify the analysis, we assume the jammer here is the constant jammer. The reactive jammer case can be treated similarly.

The intuition of MCR detection is that when only jammer is transmitting, the estimated MCR values are stable over a short period. In contrast, when the ongoing transmission collides with the jamming signals, the estimated MCR values will change significantly.

Considering the scenario in Fig. 2, when only the jammer is transmitting, we can compute MCR value $\varphi(i) = \frac{h_{11}}{h_{12}} = \frac{y_1(i)}{y_2(i)}$ as the Equation (1) shows. φ only depends on the channels between the jammer and the receiver, which will be stable in a short time.

When the transmitter TX starts to transmit, the received signals y_1 and y_2 contain both jamming and the transmitter's signals, as shown by Equation (2). If the receiver uses the same way (i.e., Equation (1)) to compute the MCR value, then the MCR value of the k-th sample becomes

$$\varphi(k) = \frac{h_{11}e^{j2\pi\Delta f_j t_k} \cdot j(k) + h_{21}e^{j2\pi\Delta f t_k} \cdot x(k)}{h_{12}e^{j2\pi\Delta f_j t_k} \cdot j(k) + h_{22}e^{j2\pi\Delta f t_k} \cdot x(k)}.$$

The stability of MCR is disrupted by the transmitter's signal components (i.e., $h_{21}e^{j2\pi\Delta f t_k}x(k)$, $h_{22}e^{j2\pi\Delta f t_k}x(k)$). Therefore, the receiver can measure the standard deviation of φ' amplitudes and use it as an indicator. If the standard deviation is greater than a certain threshold, a jammed transmission is detected by the receiver.

Fig. 3 shows φ values obtained in our experiments. It is easy to see that when only jammer is present, MCR values are stable. On the contrary, when both the jammer and the transmitter are working, MCR values change significantly from time to time.

[2] The signal processing blocks of these two receiving antennas share the same clock source, so the frequency offsets are the same.

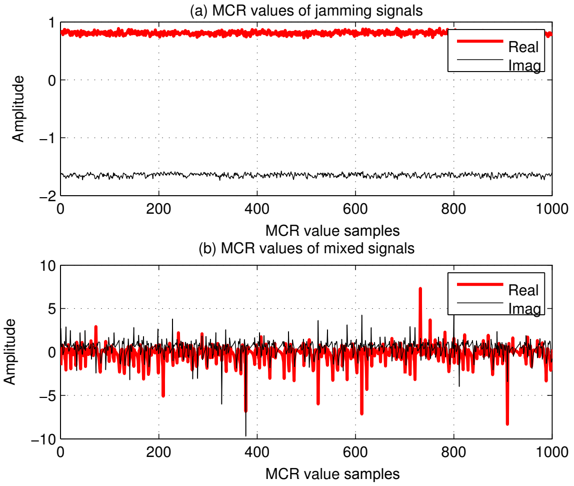

Fig. 3. MCR values. (a) shows the case when only jammer is present; (b) shows MCR values when both the transmitter and jammer are transmitting.

C. Dealing With the Constant Jammer

The constant jammer jams the channel all the time to disable any wireless communications. To defeat the constant jamming attack, the receiver can first use MCR detection to detect the transmission boundary. Then, as shown in Fig. 4, it can use the received signals which contain no transmission signals (i.e, $y_1(k), \ldots, y_1(k+l-1)$ and $y_2(k), \ldots, y_2(k+l-1)$) to compute jammer's MCR value φ, and then apply φ to remove the jamming signals in the following received signal samples. Therefore, the transmission signals can be recovered even under the jamming attack.

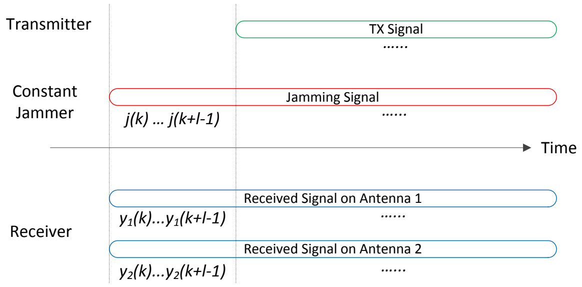

Fig. 4. Constant jamming scenario.

Note that the above discussion is for single constant jammer case. When multiple constant jammers (i.e., n jammers) exist in the network and start to jam the channel at different time, the receiver which equips $n+1$ antennas can use the above approach to remove the jamming signals from each jammer iteratively. Relevant discussion is omitted to avoid redundancy.

D. Dealing with the Reactive Jammer

For a fast reactive jammer, the reaction delay is very short, and the reactive jamming signals will always co-exist with the desired transmission signals. We term this kind of jamming attack as the fast reactive jamming attack and it cannot be defended by applying the TIMO technique. Therefore, to defeat the fast reactive jamming attack, we propose to use repeated preambles in the transmissions. As the same preamble signals will be transmitted twice, the receiver can exploit the repeated preamble signals to remove the transmission signals so that jammer's MCR can be computed.

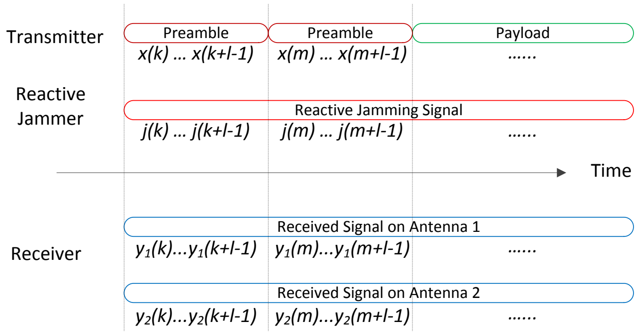

Fig. 5. Reactive jamming scenario.

As shown in Fig. 5, the reactive jamming starts and stops at the exactly the same time with the desired transmission. For the transmitted signals of the first preamble, due to the reactive jamming, the receiver obtains

$$\begin{cases} y_1(i) = h_{11}e^{j2\pi\Delta f_j t_i} \cdot j(i) + h_{21}e^{j2\pi\Delta f t_i} \cdot x(i) \\ y_2(i) = h_{12}e^{j2\pi\Delta f_j t_i} \cdot j(i) + h_{22}e^{j2\pi\Delta f t_i} \cdot x(i) \end{cases}, \qquad (3)$$

where $i \in [k, \ldots, k+l-1]$. Then, for the transmitted preamble signals of the second preamble, the receiver gets

$$\begin{cases} y_1(n) = h_{11}e^{j2\pi\Delta f_j t_n} j(n) + h_{21}e^{j2\pi\Delta f t_n} x(n) \\ y_2(n) = h_{12}e^{j2\pi\Delta f_j t_n} j(n) + h_{22}e^{j2\pi\Delta f t_n} x(n) \end{cases}, \qquad (4)$$

where $n \in [m, \ldots, m+l-1]$. The receiver needs to remove the preamble signals $x(i)$ or $x(n)$ so that it can compute the jammer's multi-channel ratio. However, due to the frequency offset, subtraction cannot be done directly [17] even though $x(i) = x(n)$. The receiver needs to find a way to compute the frequency offset by using the jammed preamble signals.

In MCR decoding, the receiver uses the Frequency-Domain Correlation and Matching technique (FDCM) [20] to get an estimation of the frequency offset. The key observation of FDCM is that the exponential change on a sequence of signals in the time domain becomes linear in the frequency domain [20]. In other words, if the receiver does a Discrete Fourier Transform (DFT) on the l received preamble signals, due to the frequency offset Δf, all the DFT values will be shifted by Δf. Thus, by correlating the original DFT values and the shifted values, Δf can be estimated by finding the correlation peak. As the DFT also has the linearity property, this approach can get the Δf even if the received signals are the mixture of the preamble signals and the jamming signals. After getting Δf, the receiver can multiple Equation (4) by $\alpha = e^{j2\pi\Delta f(t_i - t_n)}$ and subtract Equation (4) from Equation (3) to remove $x(i)$ and $x(n)$, then we have

$$\begin{cases} y_1(i) - \alpha y_1(n) = h_{11}[e^{j2\pi\Delta f_j t_i} j(i) - e^{j2\pi\Delta f_j t_n} \alpha j(n)] \\ y_2(i) - \alpha y_2(n) = h_{12}[e^{j2\pi\Delta f_j t_i} j(i) - e^{j2\pi\Delta f_j t_n} \alpha j(n)] \end{cases}.$$

Consequently, the jammer's MCR can computed as

$$\phi = \frac{h_{11}}{h_{12}} = \frac{y_1(i) - \alpha y_1(n)}{y_2(i) - \alpha y_2(n)}.$$

The computed MCR value ϕ can be used for removing the jamming signal components in the following received jammed signals.

V. Analysis

In this section, we first analyze the processing gain of MCR decoding, then discuss bit error rate of the receiver when different percentage of jamming power is removed.

A. *MCR Processing Gain*

By removing the jamming signal power, MCR decoding provides the processing gain for the multi-antenna devices. Assume x is the percentage of the jamming signal power which is removed by MCR decoding, and G_m is the MCR processing gain, then we have

$$G_m = \frac{1}{1-x}.$$

In our experiments, MCR decoding can remove more than 99.86% of the jamming signal power, then we can derive that $G_m = 28.5\ dB$. Note that when working with other anti-jamming schemes (e.g., DSSS), the MCR processing gain can add up with other processing gains. In other words, MCR decoding provides $28.5\ dB$ extra anti-jamming capacity in addition to other anti-jamming schemes, which can be used to defeat the high power jamming attacks.

B. *Bit Error Rate Analysis*

Here we assume that the receiver only uses MCR decoding for anti-jamming. We use the bit error rate of the receiver to measure the effectiveness of MCR decoding against jamming attacks.

Let us first clarify some notations. We denote the power of received jamming signal, received transmission signal and noise are J, R and N respectively. Thus, the jamming to signal power ratio is $JSR = \frac{J}{R}$, the signal to noise ratio is $SNR = \frac{R}{N}$.

According to [5], the bit error rate (BER) of a wireless device is dependent on its SNR and the modulation method, as x percent of the jamming signal power can be removed by MCR decoding, then we can derive the BER for binary phase shift keying (BPSK) as

$$P_e = Q(\sqrt{\frac{2}{\frac{1}{SNR} + JSR(1-x)}}),$$

where $Q(\cdot)$ is the Q-function [2].

Fig. 6 gives the BER values w.r.t. x and JSR (with sufficient SNR, $\frac{1}{SNR}$ is close-to-0). It is generally agreed that a packet can be received correctly when its BER is less than 10^{-3} [7], then from Fig. 6, we can see that when $x = 99.85\%$, the packets can be received correctly even though the jamming signal is $21\ dB$ stronger than the transmission signal, as the vast majority of the jamming power is removed. Note that we use BPSK for modulation in the analysis, the results for other modulation methods can be derived similarly.

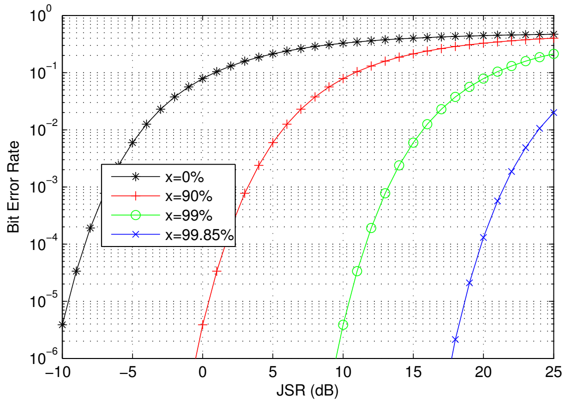

Fig. 6. Bit error rate under different jamming power removal rates.

VI. Experimental Evaluation

We have built a prototype for MCR decoding based on GNURadio and the USRP platform, and performed the real world experiments to validate our proposed techniques. In our experiments, we first validate the accuracy of MCR detection, then evaluate the removal of the jamming signal.

A. *Prototype Setup*

Hardware Configuration: The prototype system consists of a jammer, a transmitter, and a MIMO receiver; the jammer and transmitter are implemented using the USRP-N210 board connected to a host laptop via 1 Gbps Ethernet cable. The MIMO receiver is built by connecting two USRP-N210 boards with a MIMO cable. The USRP-N210 board uses a XCVR2450 daughter board operating on the 2.4GHz band as its RF front end. The MIMO receiver is about two meters away from the jammer and the transmitter.

Software Configuration: The jamming symbol rate for the jammer is 5×10^5 samples per second (sps). The transmitter and the receiver use the differential binary phase shift keying for modulation and use both GNURadio and MATLAB for signal processing.

B. *Evaluation*

1) Transmission Detection: In the experiments, we first start the jammer and the transmitter, adjust their gains to achieve $0\ dB$, $5\ dB$, $10\ dB$, $15\ dB$ and $20\ dB$ JSR. The jammer keeps on jamming the channel while the transmitter is transmitting. Then we start the MIMO receiver, which samples the wireless channel at a rate of 10^6 sps and saves the samples in a file for subsequent processing.

We use the standard deviation of 500 MCR values' amplitudes to detect ongoing transmissions. By choosing different threshold values, we get the true positive and false positive rates of MCR detection as shown in Fig. 7. Here true positive means there is a transmission and the receiver detects it; while false positive means there is no transmission, but the receiver detects one mistakenly. It is easy to see that there is a range of threshold values which allow the transmissions to be detected almost 100% with close-to-0 false positive rate, even when the jamming signal strength is 20 dB stronger than the desired transmission signal strength. Therefore, the proposed MCR detection can detect the desired transmission accurately under jamming attacks.

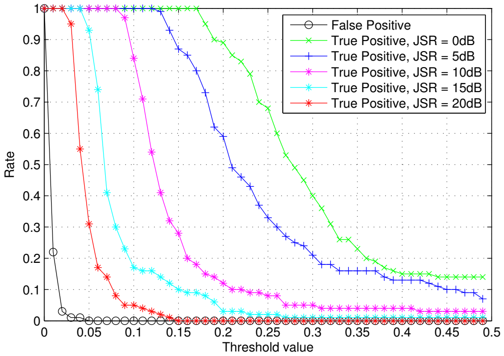

Fig. 7. False positive and true positive rates. The false positive rate is the detection rate when there are no transmissions. True positive rate is the detection rate when there is an ongoing transmission.

2) The Removal of Jamming Signal: In this part of experiments, we evaluate the jamming signal removing performance. We only start the jammer and the receiver. The jammer jams the channel all the time. The receiver first records the received jamming signals into a file, uses the first 1000 signal samples to compute the MCR value of the jammer, and then use the computed MCR to eliminate the jamming signals in the following signal samples.

In our experiments, the percentage of jamming power that can be removed by MCR decoding depends on how many samples we need to apply the elimination. The reason is that the channels between the jammer and receiver are changing slightly over time. If we apply the same MCR value to do elimination on too many samples, the difference between the MCR value we use and the real MCR value will become larger, thus less jamming power can be removed. Fig. 8 shows that when the sample number is from $1,000$ to $15,000$, more than 99.86% jamming signal power is removed. In other words, the vast majority of the jamming signal power can be effectively removed by MCR decoding.

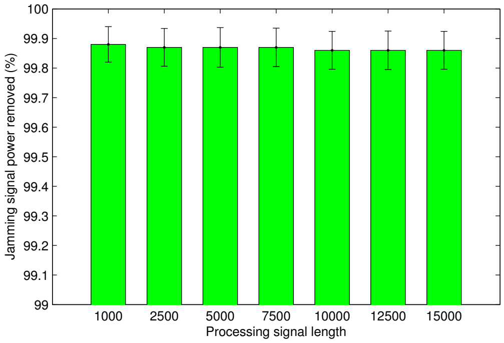

Fig. 8. Jamming power removed by MCR decoding.

VII. Conclusion

In this paper, we present MCR decoding, a technique aiming at providing an anti-jamming wireless communication capability for multi-antenna wireless devices. To perform MCR decoding, the receiver monitors the change of MCR values to detect the jammed ongoing transmission, then applies the jammer's MCR value to remove the jamming signals. We have implemented and evaluated MCR decoding on GNURadio and USRP. Our experiment results show that MCR decoding can detect the desired transmission reliably under jamming attacks and remove more than 99.86% of the jamming signal power in the real world environment.

References

[1] GNU Radio - The GNU Software Radio. http://gnuradio.org/redmine/projects/gnuradio/wiki.

[2] Q-function. http://en.wikipedia.org/wiki/Q-function.

[3] P. Castoldi. *Multiuser detection in CDMA mobile terminals*. Artech house Publishers, 2002.

[4] D. Gesbert, M. Shafi, D. Shiu, P.J. Smith, and A. Naguib. From theory to practice: an overview of MIMO space-time coded wireless systems. *IEEE JSAC*, 2003.

[5] A. Goldsmith. *Wireless communications*. Cambridge University Press, 2005.

[6] S. Gollakota, F. Adib, D. Katabi, and S. Seshan. Clearing the RF smog: Making 802.11 robust to cross-technology interference. In *SIGCOMM*, 2011.

[7] S. Gollakota and D. Katabi. Zigzag decoding: Combating hidden terminals in wireless networks. In *SIGCOMM*, 2008.

[8] R.C.T. Lee, M.C. Chiu, and J.S. Lin. *Communications engineering: Essentials for computer scientists and electrical engineers*. John Wiley & Sons, 2007.

[9] A. Liu, P. Ning, H. Dai, and Y. Liu. USD-FH: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure. In *MASS*, 2010.

[10] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang. Defending DSSS-based broadcast communication against insider jammers via delayed seed-disclosure. In *ACSAC*, 2010.

[11] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In *INFOCOM*, 2010.

[12] Ettus Research LLC. The USRP Product Family Products and Daughter Boards. http://www.ettus.com/products.

[13] R.G. Lyons. *Understanding digital signal processing*. Prentice Hall, 2011.

[14] H. Meyr, M. Moeneclaey, and S.A. Fechtel. *Digital communication receivers : synchronization, channel estimation, and signal processing*. John Wiley & Sons, 1998.

[15] C. Pöpper, M. Strasser, and S. Čapkun. Anti-jamming broadcast communication using uncoordinated spread spectrum techniques. *IEEE JSAC*, 2010.

[16] J.G. Proakis and M. Salehi. *Digital communications*. McGraw-hill, 2008.

[17] W. Shen, P. Ning, X. He, and H. Dai. Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In *IEEE Symposium on Security and Privacy*, 2013.

[18] M. Strasser, C. Pöper, S. Čapkun, and M. Čagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In *IEEE Symposium on Security and Privacy*, 2008.

[19] K. Tan, H. Liu, J. Fang, W. Wang, J. S. Zhang, M. Chen, and G. M. Voelker. SAM: Enabling practical spatial multiple access in wireless LAN. In *MobiCom*, 2009.

[20] S. Yoon, B. Jung, K Lee, and I. Rhee. Adopt: Practical add-on MIMO receiver for concurrent transmissions. Technical report, NCSU, 2012.